UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,137	08/11/2000	Michel Maillard	11345.023001	8272

22511 7590 05/31/2006

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/622,137	MAILLARD ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4-20 and 30-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4-20 and 30-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 4-20, and 30-36 are pending in this office action, claim 36 is newly added

2. Applicant's arguments, filed March 2, 2006, have been considered and are persuasive. However, a new ground of rejection has been made.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 4-8, 14-16, 30-32, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamperman (U.S. Patent No. 5,991,400) in view of Tsukamoto et al. (U.S. Patent No. 5,796,828).

Regarding claim 30, Kamperman teaches a method of recording transmitted digital data, comprising:

- Encrypting transmitted digital information of the transmitted digital data by a recording encryption key (col. 4, lines 49-54 and col. 5, lines 31-40), wherein the transmitted digital information comprises a control word (col. 4, lines 36-43);

- Storing the encrypted transmitted digital information by a recording means on a recording support medium (col. 5, lines 53-64);
- Encrypting the recording encryption key by a recording transport key (col. 6, lines 48-61); and
- Storing the encrypted recording encryption key to the recording support medium (col. 6, lines 54-57), wherein at least one of the recording encryption key and recording transport key is stored on a portable security module associated with the recording means (fig. 1, SCD, col. 5, lines 47-50, and col. 6, lines 38-41).

Kamperman does not teach encrypting transmitted data. That is, Kamperman does not teach that the encrypting is performed on data that is already transmitted, but rather the data is encrypted and then transmitted. The EMM is the recording transport key; the ECM is the recording encryption key. The decryption of the EMM provides the AK, which is used for decrypting the ECM, which provides the CW.

Tsukamoto et al. teaches an enciphering element in the set-top box that encrypts the already transmitted data for storage on a portable recording medium (fig. 2, ref. num 22 within 102A and 104A).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the already transmitted data for storage on a recording medium in the receiving end, as taught by Tsukamoto et al., with the

method of Kamperman. It would have been obvious for such modifications because the data obtained for viewing pleasure can then be securely stored within a set-top box for later viewing without the threat of having the data hacked and played on a different set-top box (see col. 5, lines 41-65).

Regarding claim 31, Kamperman teaches a system for recording transmitted digital data, comprising:

- A receiver/decoder for at least receiving the encrypted transmitted digital data (fig. 1, RE), wherein the encrypted transmitted digital data comprises a control word (col. 4, lines 36-43), and wherein the transmitted digital data is encrypted using a recording encryption key (col. 4, lines 49-54 and col. 5, lines 31-40); and
- A recording means for recording the encrypted transmitted digital data to a recording support medium, along with an encrypted recording encryption key (fig. 1, VTR),
    - Wherein the recording encryption key is encrypted via a recording transport key to obtain the encrypted recorded encryption key (col. 6, lines 48-61).

Kamperman does not teach encrypting transmitted data. That is, Kamperman does not teach that the encrypting is performed on data that is already transmitted, but rather the data is encrypted and then transmitted. The EMM is the recording transport

key; the ECM is the recording encryption key. The decryption of the EMM provides the AK, which is used for decrypting the ECM, which provides the CW.

Tsukamoto et al. teaches an enciphering element in the set-top box that encrypts the already transmitted data for storage on a portable recording medium (fig. 2, ref. num 22 within 102A and 104A).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the already transmitted data for storage on a recording medium in the receiving end, as taught by Tsukamoto et al., with the system of Kamperman. It would have been obvious for such modifications because the data obtained for viewing pleasure can then be securely stored within a set-top box for later viewing without the threat of having the data hacked and played on a different set-top box (see col. 5, lines 41-65).

Regarding claim 34, Kamperman teaches a system for recording transmitted digital data, comprising:

- A recording support medium configured to store the encrypted transmitted digital data and an encrypted recording encryption key (fig. 1, VTR, col. 5, lines 53-64 and col. 6, lines 54-57), wherein the encrypted transmitted digital data comprises a control word (col. 4, lines 36-43), wherein the transmitted digital data is encrypted using a recording encryption key (col. 4, lines 49-54 and col. 5, lines

31-40), and wherein the encrypted recording encryption key is encrypted using a recording transport key (col. 6, lines 48-61); and

- A portable security module configured to store at least one of the recording encryption key and the recording transport key (fig. 1, SCD, col. 5, lines 47-50 and col. 6, lines 38-41).

Kamperman does not teach encrypting transmitted data. That is, Kamperman does not teach that the encrypting is performed on data that is already transmitted, but rather the data is encrypted and then transmitted. The EMM is the recording transport key; the ECM is the recording encryption key. The decryption of the EMM provides the AK, which is used for decrypting the ECM, which provides the CW.

Tsukamoto et al. teaches an enciphering element in the set-top box that encrypts the already transmitted data for storage on a portable recording medium (fig. 2, ref. num 22 within 102A and 104A).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the already transmitted data for storage on a recording medium in the receiving end, as taught by Tsukamoto et al., with the system of Kamperman. It would have been obvious for such modifications because the data obtained for viewing pleasure can then be securely stored within a set-top box for later

viewing without the threat of having the data hacked and played on a different set-top box (see col. 5, lines 41-65).

Regarding claim 35, Kamperman teaches a recording support medium, comprising:

- Transmitted digital data, wherein the transmitted digital data is encrypted using a recording encryption key (col. 4, lines 49-54 and col. 5, lines 31-40), and wherein the transmitted digital data comprises a control word (col. 4, lines 36-43); and
- An encrypted recording encryption key, wherein the encrypted recording encryption key is encrypted using a recording transport key (col. 6, lines 48-61).

Kamperman does not teach encrypting transmitted data. That is, Kamperman does not teach that the encrypting is performed on data that is already transmitted, but rather the data is encrypted and then transmitted. The EMM is the recording transport key; the ECM is the recording encryption key. The decryption of the EMM provides the AK, which is used for decrypting the ECM, which provides the CW.

Tsukamoto et al. teaches an enciphering element in the set-top box that encrypts the already transmitted data for storage on a portable recording medium (fig. 2, ref. num 22 within 102A and 104A).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the already transmitted data for storage on a recording medium in the receiving end, as taught by Tsukamoto et al., with the support medium of Kamperman. It would have been obvious for such modifications because the data obtained for viewing pleasure can then be securely stored within a set-top box for later viewing without the threat of having the data hacked and played on a different set-top box (see col. 5, lines 41-65).

Regarding claim 36, Kamperman teaches a receiver/decoder used in a conditional access digital television system, comprising:

- Means for receiving encrypted transmitted digital data, wherein the encrypted transmitted digital data comprises a control word (col. 4, lines 36-43 and fig. 1, RE),
- Wherein the transmitted digital data is encrypted using a recording encrypted key (col. 4, lines 49-54 and col. 5, lines 31-40),
- Wherein the recording encryption key is encrypted via a recording transport key to obtain an encrypted recorded encryption key (col. 6, lines 48-61), and
- Wherein the receiver/decoder is operatively connected to a recording means for recording the encrypted transmitted digital data and the encrypted recording encryption key to a recording support medium (fig. 1, VTR, SCD).

Kamperman does not teach encrypting transmitted data. That is, Kamperman does not teach that the encrypting is performed on data that is already transmitted, but rather the data is encrypted and then transmitted. The EMM is the recording transport key; the ECM is the recording encryption key. The decryption of the EMM provides the AK, which is used for decrypting the ECM, which provides the CW.

Tsukamoto et al. teaches an enciphering element in the set-top box that encrypts the already transmitted data for storage on a portable recording medium (fig. 2, ref. num 22 within 102A and 104A).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the already transmitted data for storage on a recording medium in the receiving end, as taught by Tsukamoto et al., with the receiver/decoder of Kamperman. It would have been obvious for such modifications because the data obtained for viewing pleasure can then be securely stored within a set-top box for later viewing without the threat of having the data hacked and played on a different set-top box (see col. 5, lines 41-65).

Regarding claim 4, Kamperman as modified by Tsukamoto et al. teaches the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means (see fig. 1, TE, SCR & RE, DSC of Kamperman).

Regarding claim 5, Kamperman as modified by Tsukamoto et al. teaches the decoder is associated with a portable security module used to store transmission access control keys (KO (NS), KO' (Op1, NS) etc.) used to decrypt the transmitted encrypted information (see col. 5, lines 19-31 of Kamperman).

Regarding claim 6, Kamperman as modified by Tsukamoto et al. teaches at least one of the recording encryption key (E (NE)) and/or recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (KO (NS), KO' (Op1, NS) etc.) function in accordance with a second encryption algorithm (CA) (see fig. 2A, the KRD is created differently than the AK of Kamperman).

Regarding claim 7, Kamperman as modified by Tsukamoto et al. teaches the recording transport key (RT (A)) is generated at a central recording authorization unit and a copy of this key communicated to the recording means (see col. 6, lines 10-20 of Kamperman).

Regarding claim 8, Kamperman as modified by Tsukamoto et al. teaches the recording transport key (RT (A)) is encrypted by a further encryption key (KO (NSIM)) prior to being communicated to the recording means (see col. 6, lines 48-57 of Kamperman).

Regarding claim 14, Kamperman as modified by Tsukamoto et al. teaches:

- Using a decoder means and associated security module and a recording means and associated security module (see fig. 1, VTR, SCD, RE of Kamperman) and
- In which a copy of the recording transport key (RT (A)) is stored in at least one of the security module associated with the decoder means and/or the security module associated with the recording means (see col. 6, lines 54-57 of Kamperman).

Regarding claim 15, Kamperman as modified by Tsukamoto et al. teaches the recording transport key (RT (A)) is generated by either the recording security modules or decoder security module and communicated to the other security module (see fig. 1, SCD sends the KRD to the VTR of Kamperman).

Regarding claim 16, Kamperman as modified by Tsukamoto et al. teaches the recording transport key (RT (A)) is encrypted before communication to the other security module and decrypted by a key unique (KO (NS)) to that other security module (see col. 6, lines 48-65 of Kamperman).

Regarding claim 32, Kamperman as modified by Tsukamoto et al. teaches further comprising a decoder means and associated security module adapted to store a copy of the recording transport key (RT(A)) (see fig. 1, VTR, SCD, RE of Kamperman).

Claims 9-13 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamperman (USPN '400) in view of Tsukamoto et al. (USPN '828), and further in view of Bednarek et al. (U.S. Patent No. 5,621,793).

Regarding claim 9, Kamperman as modified by Tsukamoto et al. teaches all of the subject matter of claim 1, as discussed above. However, Kamperman as modified by Tsukamoto et al. does not disclose a central access control system communicates transmission access control keys (KO (NS), KO' (Op 1, NS) etc.) to the recording means.

Bednarek et al. teaches a central access control system communicates transmission access control keys (KO (NS), KO' (Op 1, NS) etc.) to the recording means (col. 8, line 61 through col. 9, line 13).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a central access control system communicates keys to the recording means, as taught by Bednarek et al., to the method of Kamperman/Tsukamoto et al. It would have been obvious for such modifications because the central access provides the keys needed for descrambling; this prevents tampering with the set-top box because the keys are not stored therein.

Regarding claim 10, Kamperman as modified by Tsukamoto et al./Bednarek et al. teaches the transmission access control keys (KO (NS), KO' (Op1, NS) etc.) are communicated to a portable security module associated with the recording means (see col. 13, lines 31-51 of Bednarek et al.).

Regarding claims 11 and 33, Kamperman as modified by Tsukamoto et al./Bednarek et al. teaches the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium (see fig. 2, ref. num 46 of Bednarek et al.).

Regarding claim 12, Kamperman as modified by Tsukamoto et al./Bednarek et al. teaches central access control system encrypts the broadcast access control keys (KO (NS), KO' (Op1, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means (see col. 6, lines 28-60 of Bednarek et al.).

Regarding claim 13, Kamperman as modified by Tsukamoto et al./Bednarek et al. teaches the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request being authenticated by the recording means using a key (KO (NSIM)) unique to that recording means (see col. 5, lines 19-34 of Bednarek et al.).

Claims 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamperman (USPN '400) in view of Tsukamoto et al. (USPN '828), and further in view of Park (European Patent No. 714204).

Regarding claim 17, Kamperman as modified by Tsukamoto et al. teaches all of the subject matter of claims 1 and 14-16, as discussed above. However, Kamperman as modified by Tsukamoto et al. does not disclose the decoder security module and recording security module (52) carry out a mutual authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization.

Park teaches the decoder security module and recording security module (52) carry out a mutual authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization (page 8, lines 43-45).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine mutual authorization between the security module and recording module, as taught by Park, to the method of Kamperman/Tsukamoto et al. It would have been obvious for such modifications because mutual authorization ensures integrity between the two devices.

Regarding claim 18, Kamperman as modified by Tsukamoto et al./Park teaches the mutual authorization step is carried out using, inter alia, an audience key KI (C) known to both security modules (30,52) (see page 8, lines 39-42 of Park).

Regarding claim 19, Kamperman as modified by Tsukamoto et al. teaches all of the subject matter of claims 1 and 14, as discussed above. However, Kamperman as modified by Tsukamoto et al. does not disclose the decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)).

Park teaches:

- The decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form (page 8, lines 10-19) and
- A session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)) (page 8, lines 20-22).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key, as taught by Park, to the method of Kamperman/Tsukamoto et al. It would have been obvious for such modifications because the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form would allow the security module to properly decrypt the encrypted data for proper restoration of the signal. Also, a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key would secure the clear signal again before transmission to the recording device, thus making the secure digital recording device more secure.

Regarding claim 20, Kamperman as modified by Tsukamoto et al./Park teaches the session key (K3 (NSIM)) is generated by one of the decoder security module or recording means security module and communicated to the other module in encrypted form using an encryption key (KO (NS)) uniquely decryptable by the other security module (see page 8, lines 20-22 of Park).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100